TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN FÜR GOTO MEETING, GOTO WEBINAR, GOTO TRAINING UND GOTO STAGE

Dokumentation zu organisatorischen Sicherheits- und Datenschutzkontrollen

Datum der Veröffentlichung: Februar 2022

1 Produkte und Dienste

Dieses Dokument behandelt die technischen und organisatorischen Maßnahmen (TOMs) für GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage (gemeinsam als „GoTo-UCC-Lösungen“ bezeichnet).

Bei den GoTo-UCC-Lösungen handelt es sich um Online-Kommunikationsdienste, die es Einzelpersonen und Unternehmen ermöglichen, über verschiedene Funktionen zu interagieren, die je nach Dienstangebot die Desktop-Bildschirmübertragung, Videokonferenzen und integrierte Audiofunktionen umfassen können. Die Dienste der GoTo-UCC-Lösungen werden mittels eines Webbrowsers oder eines Client-Programms über ein global verteiltes Netzwerk proprietärer Hardware und Software bereitgestellt.

- GoTo Meeting ermöglicht es Nutzern, über die GoTo Meeting-Website und/oder die Client-Software Meetings zu planen, einzuberufen und zu moderieren.
- GoTo Webinar ermöglicht es Unternehmen, über das Internet Events und Präsentationen für ein größeres lokales oder globales Publikum durchzuführen. Webinare werden über die GoTo-Webinar-Website und/oder die Client-Software geplant, einberufen und moderiert.
- GoTo Training ermöglicht es Nutzern, Schulungssitzungen über die GoTo-Training Website und/oder über Client-Software zu planen, einzuberufen und zu moderieren. Die Lösung stellt spezielle Funktionen für webbasierte Schulungen bereit, wie z. B. Online-Zugang zu Tests und Schulungsmaterialien und ein gehostetes Kursverzeichnis.
- GoTo Stage ist ein Online-Portal, auf dem GoTo-Webinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo-Stage-Homepage vorgestellt. Organisatoren können die Veröffentlichung ihrer Aufzeichnung jederzeit über GoTo Webinar rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoTo-Stage-Umgebung gelöscht werden.

2 Produktarchitektur

Die Bildschirmübertragung zwischen den Teilnehmern in einer Sitzung einer GoTo-UCC-Lösung erfolgt über einen Overlay-Netzwerkstapel, der logisch über dem konventionellen TCP/IP-Stapel auf den Computern der einzelnen Benutzer angeordnet ist (siehe Abbildung 1).

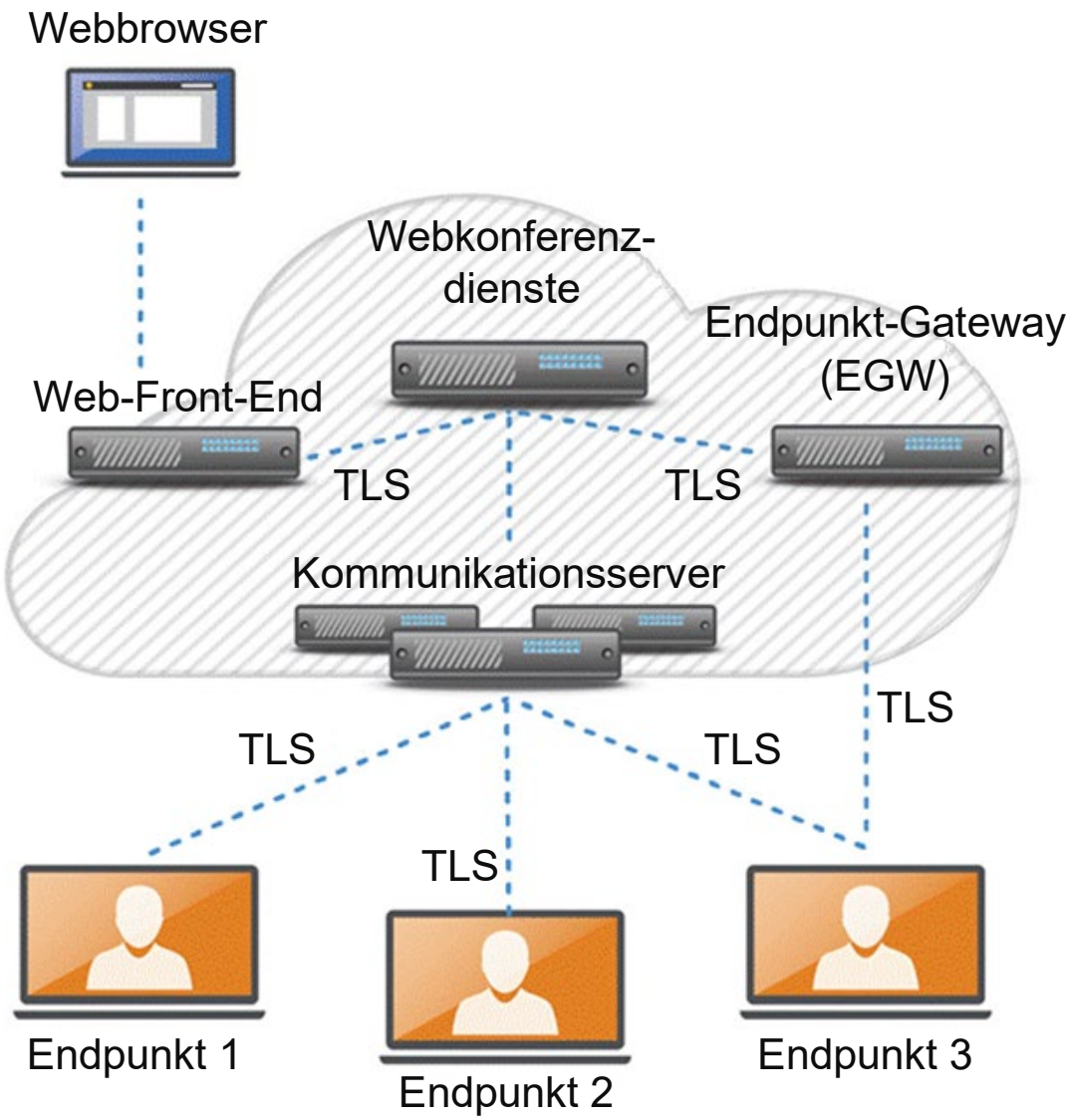

Abbildung 1 – Architektur von GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage

***Web-Front-End** – Portal-Website der GoTo-Suite; gehostet in Tier-1-Colocation-Rechenzentren und auf AWS*

***WCS** – Sitzungsplanung; Meeting-Chronik; GTM-Organisatoreinstellungen; gehostet in Tier-1-Colocation-Rechenzentren*

***Kommunikationsserver** – inkl. Bildschirmübertragungsserver, Audiobrücken und Voice-Gateways (agiert als Proxy), H.323-Gateways – gehostet auf Amazon Web Services / **Multicast-Kommunikations-server** und Video Cluster Server werden in Tier-1-Colocation-Rechenzentren gehostet*

***Endpunkt-Gateway (EGW)** – verwaltet die Verbindungen zwischen dem Organisator und den Teil-nehmerendpunkten sowie das Verschlüsselungsverfahren – EGW wird auf Amazon Web Services gehostet*

Die Teilnehmer (Sitzungsendpunkte) verwenden ausgehende TCP/IP-Verbindungen über den Port 443, um mit den Kommunikationsservern und Gateways der Infrastruktur zu kommunizieren, wobei sich die Teilnehmer überall im Internet befinden können. Clients kommunizieren mit GoTo-UCC-Lösungen in der Regel über das Endpunkt-Gateway. Neue Clients kommunizieren jedoch direkt über REST-Aufrufe (Representational State Transfer) mit den

Backend-Diensten mittels Load Balancer. Die Dienstinfrastruktur ermöglicht es auch Benutzern des öffentlichen Telefonnetzes (PSTN), sich in ein Meeting einzuwählen.

Die GoTo-UCC-Lösungen verwenden ein ASP-Modell (Application Service Provider), das für einen sicheren Betrieb sorgt und sich dabei in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt.

Die Architektur ist auf hohe Leistung, Zuverlässigkeit und Skalierbarkeit ausgelegt und wird von leistungsstarken Servern und Netzwerkgeräten mit entsprechenden Sicherheitspatches betrieben. Redundante Switches und Router sind so konzipiert, dass es keinen „Single Point of Failure“ geben kann. Geclusterte Server und Backup-Systeme sollen die Anwendungsprozesse im Falle einer hohen Auslastung oder eines Systemausfalls sicherstellen. Webkonferenzdienste verteilen für eine optimale Leistung und angemessene Latenz die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikationsserver.

Die Dienstinfrastruktur wird hauptsächlich in Tier-1-Colocation-Rechenzentren gehostet, wobei einige Dienstkomponenten bei Cloud-Hosting-Anbietern gehostet werden. Die Audiobrückendienste werden vollständig bei Cloud-Anbietern gehostet, während einige der Webkonferenzdienste der Produkte bei Cloud-Anbietern gehostet werden. Die Daten, die mit einem bei einem Cloud-Anbieter gehosteten Dienst verbunden sind, werden auch bei diesem Anbieter gespeichert.

Der physische Zugang zu den gehosteten Colocation-Servern ist beschränkt und wird kontinuierlich überwacht. Alle Standorte verfügen über redundante Stromversorgungen und Einrichtungen zur Kontrolle der Umgebungsbedingungen. Die privaten Netzwerke und Backend-Server von GoTo sind durch Firewalls, Router und VPN-basierte Zugangskontrollen gesichert. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und unabhängige, externe Prüfer führen regelmäßige Tests auf Schwachstellen durch.

Weitere Informationen finden Sie im UCC Security White Paper (UCC-Sicherheits-Whitepaper).

3 Technische Sicherheitskontrollen der GoTo-UCC-Lösungen

GoTo setzt branchenübliche technische Kontrollen ein, die der Art und dem Umfang der Dienste (wie in den Nutzungsbedingungen definiert) angemessen sind, um die Infrastruktur der Dienste und die darin enthaltenen Daten zu schützen. Die Nutzungsbedingungen finden Sie unter https://www.goto.com/company/legal/terms-and-conditions.

3.1. Logische Zugriffskontrolle

Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollverfahren sollen die Bedrohungen des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden. Mitarbeitern wird nach Bedarf minimaler Zugriff (oder „geringste Rechte“) auf bestimmte GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte gewährt. Außerdem werden die Berechtigungen der Benutzer je nach funktionaler Rolle und Umgebung getrennt.

3.2. Perimeterabwehr und Erkennung von Eindringversuchen

GoTo setzt branchenübliche Perimeterabwehr-Tools, Techniken und Dienste zum Schutz des Perimeters ein, die verhindern sollen, dass nicht autorisierter Netzwerk-Datenverkehr in unsere Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch hostbasierte Firewalls. Darüber hinaus wird ein cloudbasierter DDoS-Präventionsdienst eines Drittanbieters zum Schutz vor volumetrischen DDoS-Angriffen eingesetzt, der mindestens einmal pro Jahr getestet wird. Kritische Systemdateien werden vor böswilliger und unbeabsichtigter Infektion oder Zerstörung geschützt.

3.3. Datentrennung

GoTo nutzt eine logisch auf Datenbankebene getrennte Multi-Tenant-Architektur, die auf dem GoTo-Konto eines Benutzers oder einer Organisation basiert. Nur authentifizierte Parteien erhalten Zugriff auf die entsprechenden Konten.

3.4. Physische Sicherheit

Physische Sicherheit im Rechenzentrum

GoTo schließt Verträge mit Rechenzentren ab, um die physische Sicherheit und Umgebungskontrollen für Serverräume zu gewährleisten, in denen Produktionsserver untergebracht sind. Zu diesen Kontrollen gehören die folgenden:

- Videoüberwachung und -aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- HLK-Temperaturregelung (Heizung, Lüftung und Klimatisierung)
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (UPS)
- Doppelböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen natürlichen und vom Menschen verursachten Katastrophen, je nach Geografie und Standort des jeweiligen Rechenzentrums
- Planmäßige Wartung und Validierung aller kritischen Sicherheits- und Umgebungskontrollen

GoTo beschränkt den physischen Zugang zu den Produktionsdatenzentren auf autorisierte Personen. Um Zugang zu einer Hosting-Einrichtung zu erhalten, muss ein Antrag über das entsprechende Ticketsystem gestellt werden, der vom zuständigen Manager genehmigt und vom technischen Betriebsteam überprüft und genehmigt werden muss. Das GoTo-Management überprüft mindestens vierteljährlich die Protokolle des physischen Zugangs zu den Rechenzentren und Serverräumen. Außerdem wird der physische Zugang zu den Rechenzentren widerrufen, wenn ein zuvor autorisierter Mitarbeiter entlassen wird.

3.5. Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von GoTo ist im Allgemeinen so konzipiert, dass eine Replikation in nahezu Echtzeit an geografisch verteilten Standorten erfolgt. Datenbanken werden mit einer rollierenden inkrementellen Backup-Strategie gesichert. Im Notfall oder bei einem Totalausfall an einem der zahlreichen aktiven Standorte sind die verbleibenden Standorte so konzipiert, dass sie die Anwendungslast ausgleichen. Die Notfallwiederherstellung dieses Systems wird regelmäßig getestet.

3.6. Schutz vor Malware

Auf allen Servern der GoTo-UCC-Lösungen ist eine Malware-Schutzsoftware mit Audit-Protokollierung installiert. Alarme, die auf potenzielle bösartige Aktivitäten hinweisen, werden an das entsprechende Reaktionsteam weitergeleitet.

3.7. Vertraulichkeit und Authentizität der Daten

GoTo nutzt einen kryptografischen Standard, der den Empfehlungen von Branchenverbänden, behördlichen Veröffentlichungen und anderen einschlägigen Standardverbänden entspricht. Der kryptografische Standard wird regelmäßig überprüft, und die ausgewählten Technologien und Verschlüsselungsverfahren können je nach Risikobewertung und Marktakzeptanz neuer Standards aktualisiert werden.

3.7.1. Daten während der Übertragung

GoTo Meeting, GoTo Webinar und GoTo Training bieten Sicherheitsmaßnahmen für Daten während der Übertragung, die zur Abwehr von passiven und aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten konzipiert sind. Bildschirm- und Videoübertragungen, VoIP, Webcam-Video, Tastatur-/Maussteuerung und Text-Chat-Informationen (jeweils „Sitzungsdaten“) verfügen über branchenübliche Sicherheitskontrollen für die Kommunikation.

Sitzungsdaten werden bei der Übertragung zwischen den Endpunkten und den Kommunikationsservern von GoTo niemals in Klartext offengelegt.

In zwei Schichten sind Kommunikationssicherheitskontrollen auf Basis starker Verschlüsselung implementiert: (i) über dem Transmission Control Protocol (TCP) und dem User Datagram Protocol (UDP) und (ii) im Multicast Packet Security Layer (MPSL).

TCP- und UDP-Sicherheit

Zum Schutz der TCP-Kommunikation zwischen Endpunkten werden TLS-Standardprotokolle (Transport Layer Security) der Internet Engineering Task Force (IETF) verwendet.

Zu ihrer eigenen Sicherheit empfiehlt GoTo seinen Kunden, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Verschlüsselung verwenden, und stets die aktuellsten Sicherheitspatches für ihr Betriebssystem und ihre Browser zu installieren.

Beim Aufbau von TLS-Verbindungen zur Website und zwischen Komponenten von GoTo Meeting, GoTo Webinar oder GoTo Training nutzen GoTo-Server Zertifikate mit öffentlichem Schlüssel, um sich bei Clients zu authentifizieren. Als zusätzlicher Schutz vor Infrastrukturattacken erfolgt eine gegenseitige zertifikatbasierte Authentifizierung bei allen Server-zu-Server-Verbindungen (z. B. zwischen Kommunikationsservern und Webkonferenzdiensten).

Für Daten, die mittels UDP gesendet werden, wird eine bestehende TLS-Verbindung genutzt, um kryptografische Schlüssel sicher auszutauschen, die zur Verschlüsselung und Authentifizierung von UDP-Daten verwendet werden.

Multicast Packet Layer Security

Multicast-Daten wie Tastatur-/Maussteuerung, Chat und Informationen zum Sitzungsstatus werden durch Verschlüsselungs- und Integritätsmechanismen während der Übertragung geschützt, die verhindern sollen, dass Personen mit Zugriff auf die Kommunikationsserver (ob mit guten oder bösen Absichten) bei einer Sitzung „mithören“ oder unerkannt Daten manipulieren können. Die MPSL bietet eine zusätzliche Ebene der Vertraulichkeit und Integrität der Kommunikation, die es nur bei GoTo-Produkten gibt. Diese zusätzliche Sicherheitsebene verwendet eine 128-Bit-AES-Verschlüsselung im Counter-Modus für zusätzlichen Schutz gegen Abhören und Manipulation.

Zur Optimierung der Bandbreite werden Klartextdaten in der Regel vor der Verschlüsselung mit proprietären, leistungsstarken Methoden komprimiert. Der Schutz der Datenintegrität wird durch Einschluss eines Integritätskontrollwerts erreicht, der derzeit mit dem HMAC-SHA-1-Algorithmus generiert wird.

Die Schlüsselvereinbarung erfolgt mittels eines zufällig generierten 128-Bit-Startwerts („Seed“), der vom GoTo-Dienst ausgewählt und über TLS an alle Endpunkte verteilt wird. Er dient als Eingabe für eine vom NIST genehmigte Schlüsselableitungsfunktion. Bei Beendigung der Sitzung wird der Seed aus dem Speicher des Dienstes gelöscht.

Sicherheit der Tonübertragung

Integrierte Audiokonferenzen für GoTo Meeting, GoTo Webinar und GoTo Training werden sowohl über das öffentliche Telefonnetz (PSTN) als auch über Voice over Internet Protocol (VoIP) bereitgestellt. Bei Verwendung des Telefonnetzes ist die Vertraulichkeit und Integrität der Sprachkommunikation bereits gewährleistet. Zum Schutz der Vertraulichkeit und Integrität der VoIP-Verbindungen zwischen den Endpunkten und den Telefonkonferenzservern kommt sowohl über UDP als auch TCP ein SRTP-basiertes Protokoll mit AES-128-HMAC-SHA1 zum Einsatz. Client und Server tauschen die Schlüssel über eine hergestellte TLS-Verbindung aus.

Sicherheit der Videoübertragung

Zum Schutz der Vertraulichkeit und Integrität von Videoverbindungen zwischen den Endpunkten und den Videoservern nutzt GoTo ein SRTP-basiertes Protokoll mit AES-128-HMAC-SHA1. Client und Server tauschen die Schlüssel über eine hergestellte TLS-Verbindung aus.

Sicherheit der Webcasts

GoTo-Webinar-Webcasts nutzen Kommunikationsserver, Broadcast-Gateways, Streaming-Engines von Drittanbietern und Content Delivery Networks, die darauf ausgelegt sind, Teilnehmern, die sich über einen Browser anmelden, zuverlässig Bildschirm-, Ton- und Videoübertragung zu ermöglichen. Die Gateways empfangen die Mediendaten von den Kommunikationsservern, transkodieren sie in Standard-Codecs und leiten sie über RTP an die Streaming-Engine weiter – alles innerhalb unseres sicheren internen Netzwerks. Die Streaming-Engine unterstützt HTTP Live Streaming (HLS) mit mehreren Bitraten, um eine adaptive Übertragung für Clients mit suboptimalen Netzwerkverbindungen zu ermöglichen. Die CDNs wurden so eingerichtet, dass sie die Daten von der Streaming-Engine sicher über https abrufen. Die Clients rufen auch die Daten von CDNs über https sicher ab.

GoTo Stage

GoTo Stage ist ein Online-Portal, auf dem GoTo-Webinar-Organisatoren anpassbare Kanäle erstellen, über die sie aufgezeichnete Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo-Stage-Homepage vorgestellt. Ein auf GoTo Stage veröffentlichtes Video kann auf der GoTo-Stage-Startseite und in den Suchmaschinenergebnissen gefunden werden, es sei denn, der Organisator schränkt die Auffindbarkeit über die administrativen Einstellungen auf seiner Kanalseite ein. Andernfalls kann jeder, der bei GoTo Stage registriert ist, die Aufzeichnung über einen direkten Link zum Kanal oder auf der individuellen „Jetzt ansehen"-Seite des Videos ansehen. Besucher registrieren sich für GoTo Stage mit ihrem Namen und ihrer E-Mail-Adresse oder können sich über ausgewählte Konten in sozialen Medien wie LinkedIn, Facebook und Gmail anmelden. Nach der Registrierung erfolgt die Wiedergabe des aufgezeichneten Webinars über eine signierte S3-URL mit einer festgelegten TTL. Organisatoren können die Veröffentlichung ihrer Aufzeichnung jederzeit über GoTo Webinar rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoTo-Stage-Umgebung gelöscht werden. Die Administrationsfunktionen von GoTo Stage sind passwortgeschützt, und alle Verbindungen im GoTo-Stage-Portal sind mit TLS geschützt.

3.7.2. Ruhende Daten

In GoTo Meeting, GoTo Webinar und GoTo Training können Organisatoren ihre Live-Sitzungen einschließlich Audio-, Video- und Bildschirminhalten aufzeichnen. Sobald ein Organisator die Aufzeichnung startet, werden die Teilnehmer dazu benachrichtigt. Dass eine Aufzeichnung läuft, wird ihnen dann auf dem Bedienpanel angezeigt. Kunden können wählen, ob sie Sitzungsaufzeichnungen auf ihrem lokalen Rechner oder in der Cloud speichern möchten.

Cloud-Aufzeichnungen

Cloud-Aufzeichnungen werden auf AWS S3 gespeichert. Die Dateien werden im Ruhezustand serverseitig mittels 256-Bit-AES verschlüsselt.

Transkripte

Wenn der Organisator dies aktiviert, wird die Speech-to-Text-Technologie von Google Cloud zur Transkription von Sitzungsaufzeichnungen verwendet. Audiodateien werden zur Transkription mit TLS übertragen, wobei die Dateien mit 256-Bit-AES verschlüsselt und sofort nach Abschluss der Speech-to-Text-Verarbeitung gelöscht werden. Die Transkripte werden von GoTo über seine AWS S3-Instanz verwaltet und dem Organisator unter „Cloud-Aufzeichnungen" zur Verfügung gestellt.

Upload von Inhalten

Einige der GoTo-Dienste bieten Organisatoren die Möglichkeit, Videos zur Verwendung in Live-Sitzungen hochzuladen. Auch diese Uploads werden in AWS S3 gespeichert und bei der Übertragung dorthin sowie bei der Speicherung mit 256-bit-AES verschlüsselt.

3.8. Schwachstellenmanagement

Interne und externe System- und Netzwerk-Schwachstellen-Scans werden einmal im Monat durchgeführt. Dynamische und statische Schwachstellenprüfungen von Anwendungen sowie Penetrationstests für bestimmte Umgebungen werden ebenfalls regelmäßig durchgeführt.

Die Ergebnisse dieser Scans und Tests werden an die Netzwerküberwachungs-Tools übergeben, und je nach Schweregrad der identifizierten Schwachstellen werden gegebenenfalls Abhilfemaßnahmen ergriffen.

Schwachstellen werden auch durch monatliche und vierteljährliche Berichte an die Entwicklungs- und Verwaltungsteams kommuniziert und verwaltet.

3.9. Protokollierung und Warnmeldungen

GoTo sammelt identifizierten anomalen oder verdächtigen Datenverkehr in den entsprechenden Sicherheitsprotokollen der jeweiligen Produktionssysteme.

4 Organisatorische Kontrollen

GoTo setzt eine umfassende Reihe von organisatorischen und administrativen Kontrollen ein, um die Sicherheit und den Datenschutz der GoTo-UCC-Lösungen zu gewährleisten.

4.1. Sicherheitsrichtlinien und -verfahren

GoTo setzt eine umfassende Reihe von Sicherheitsrichtlinien und -verfahren ein, die den Geschäftszielen, Compliance-Programmen und den Interessen der allgemeinen Unternehmensführung entsprechen. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um ihre Einhaltung zu gewährleisten.

4.2. Einhaltung von Standards

GoTo erfüllt die geltenden rechtlichen, finanziellen, datenschutzrechtlichen und regulatorischen Anforderungen und hält sich an die folgenden Zertifikate und externen Prüfberichte:

- TRUSTe Enterprise Privacy- und Data Governance Practices-Zertifizierung für betriebliche Datenschutz- und Datensicherheitskontrollen, die mit den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzrahmenwerken übereinstimmen. Um mehr zu erfahren, besuchen Sie unseren Blogbeitrag.
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Typ 2 Zertifizierungsbericht
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Typ II Zertifizierungsbericht
- Payment Card Industry Data Security Standard (PCI DSS)-Compliance für die E-Commerce- und Zahlungsumgebungen von GoTo
- Bewertung der internen Kontrollen, wie im Rahmen einer Jahresabschlussprüfung des Public Company Accounting Oversight Board (PCAOB) erforderlich

4.3. Sicherheitsmaßnamen und Incident-Management

Das Security-Operations-Team des GoTo Security Operations Centers (SOC) ist für die Erkennung von und die Reaktion auf Sicherheitsereignisse zuständig. Das SOC verwendet Sicherheitssensoren und Analysesysteme, um potenzielle Probleme zu identifizieren, und hat einen Plan zur Reaktion auf Vorfälle entwickelt, der angemessene Reaktionen vorschreibt.

Der Plan zur Reaktion auf Vorfälle ist auf die kritischen Kommunikationsprozesse von GoTo, die Richtlinie für das Management von Vorfällen im Bereich der Informationssicherheit sowie die zugehörigen Standardbetriebsverfahren abgestimmt. Diese Richtlinien und Verfahren wurden entwickelt, um mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten von GoTo, einschließlich der GoTo-UCC-Lösungen, zu verwalten, zu identifizieren und zu beheben. Gemäß dem Plan für die Antwort auf Vorfälle gibt es technische Mitarbeiter, die potenzielle Ereignisse und Schwachstellen im Zusammenhang mit der Informationssicherheit identifiziert und vermutete oder bestätigte Ereignisse gegebenenfalls an die Verwaltung weiterleitet. Mitarbeiter können Sicherheitsvorfälle per E-Mail, Telefon und/oder Ticket melden, entsprechend dem auf der GoTo-Intranetseite dokumentierten Verfahren. Alle identifizierten oder vermuteten Ereignisse werden dokumentiert und über standardisierte Ereignistickets eskaliert und nach ihrer Kritikalität eingestuft.

4.4. Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo basiert auf dem Microsoft Security Development Lifecycle (SDL), um den Produktcode zu abzusichern. Die Kernelemente dieses Programms sind manuelle Codeprüfungen, Bedrohungsmodellierung, statische Codeanalyse, dynamische Analyse und Systemhärtung.

4.5. Mitarbeitersicherheit

Hintergrundüberprüfungen werden, soweit gesetzlich zulässig und für die jeweilige Position angemessen, bei neuen Mitarbeitern vor dem Einstellungsdatum global durchgeführt. Die Ergebnisse werden in der Personalakte des Mitarbeiters hinterlegt. Die Kriterien für die Hintergrundüberprüfung hängen von den Gesetzen, der beruflichen Verantwortung und der Führungsebene des potenziellen Mitarbeiters ab und unterliegen den üblichen und angemessenen Praktiken des jeweiligen Landes.

4.6. Programme für Sicherheitssensibilisierung und -schulung

Neu eingestellte Mitarbeiter werden bei der Einarbeitung über die Sicherheitsrichtlinien und den betrieblichen Verhaltenskodex und die ethischen Grundsätze von GoTo informiert. Diese obligatorische jährliche Sicherheits- und Datenschutzschulung wird den betreffenden Mitarbeitern bereitgestellt und vom Talent-Development-Team mit Unterstützung des Sicherheitsteams verwaltet.

GoTo-Mitarbeiter und Zeitarbeitskräfte werden regelmäßig über Sicherheits- und Datenschutzleitfäden, -verfahren, -richtlinien und -standards informiert, u. a. durch Onboarding-Kits für neue Mitarbeiter, Sensibilisierungskampagnen, Webinare mit dem CISO, ein Security-Champion-Programm und mindestens halbjährlich wechselnde Poster und andere Ressourcen, die Methoden zur Sicherung von Daten, Geräten und Einrichtungen erläutern.

5 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten seiner Kunden, der Abonnenten der GoTo-UCC-Lösungen und der Endbenutzer sehr ernst und verpflichtet sich, relevante Praktiken zur Datenverarbeitung und -verwaltung offen und transparent darzulegen.

5.1. DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) über den Schutz der Daten und der Privatsphäre aller Personen in der EU. Hauptziel der DSGVO ist es, den Bürgern und Einwohnern mehr Kontrolle über ihre personenbezogenen Daten zu geben und das regulatorische Umfeld innerhalb der EU zu vereinfachen. Die GoTo-UCC-Lösungen halten die geltenden Bestimmungen der DSGVO ein. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo versichert und garantiert hiermit, dass es den California Consumer Privacy Act (CCPA) einhält. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3. Datenschutzrichtlinien

GoTo bietet einen umfassenden globalen Datenverarbeitungsnachtrag (DVN), der die Verarbeitung personenbezogener Daten durch GoTo regelt, in Englisch sowie Deutsch verfügbar ist und die Anforderungen der DSGVO, CCPA erfüllt bzw. sie übertrifft.

Der DVN schließt folgende Datenschutz-Anforderungen in Bezug auf die DSGVO ein: (a) Details zur Datenverarbeitung, Offenlegung bzgl. Auftragsverarbeiter-Partnerunternehmen etc. gemäß Artikel 28; (b) zur Regelung der gesetzeskonformen Übermittlung gemäß der DSGVO mittels Anwendung der EU-Standardvertragsklauseln (auch als EU-Modellklauseln bekannt); und (c) die technischen und organisatorischen Maßnahmen von GoTo. Im Zusammenhang mit dem CCPA haben wir zusätzlich in unserem globalen DVN Folgendes aktualisiert: (a) Definitionen im Zusammenhang mit dem CCPA; (b) Zugriffs- und Löschrechte; und (c) Garantien, dass GoTo keine persönlichen Daten von Benutzern verkaufen wird.

Für Besucher unserer Webseiten legt GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Dienste bereitzustellen, zu pflegen, zu verbessern und zu sichern, in seiner Datenschutzrichtlinie auf der öffentlichen Website offen. Das Unternehmen kann die Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen seiner Informationspraktiken und/oder Änderungen des anwendbaren Rechts zu reflektieren, wird jedoch auf seiner Website über alle wesentlichen Änderungen informieren, bevor diese in Kraft treten.

5.4. Abkommen zur Datenübertragung

GoTo verfügt über ein robustes globales Datenschutzprogramm, das die geltenden Gesetze berücksichtigt und rechtmäßige internationale Datenübertragungen unter den folgenden Rahmenbedingungen unterstützt:

5.4.1. Standardvertragsklauseln

Die Standardvertragsklauseln („SCC“) sind standardisierte Vertragsbestandteile, die von der Europäischen Kommission anerkannt und übernommen wurden und vorrangig dem Zweck dienen, eine EU-datenschutzkonforme Übermittlung personenbezogener Daten in Regionen außerhalb des Europäischen Wirtschaftsraums („EWR“) sicherzustellen. GoTo hat ein ausgefeiltes Datenschutzprogramm eingerichtet, das die Ausführungsbestimmungen der SCC für die Übermittlung personenbezogener Daten einhält. GoTo bietet Kunden SCC (andere Bezeichnung: EU-Modellklauseln) an. Diese leisten als Bestandteil des globalen DNV von GoTo spezifische Garantien be-

treffend die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen GoTo-Dienste. Der Abschluss der SCC hilft, die freie Übermittlung der Daten von GoTo-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

Zusätzlich zu den in diesen TOMs genannten Maßnahmen hat GoTo die folgenden FAQs erstellt, die die zusätzlichen Maßnahmen zur Unterstützung rechtmäßiger Übertragungen gemäß Kapitel 5 der DSGVO darlegt und alle vom Europäischen Gerichtshof in Verbindung mit der SCCs empfohlenen Einzelfallanalysen behandelt und leitet.

5.4.2. Zertifizierung nach APEC CBPR und PRP

GoTo hat außerdem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft) CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC CBPR und PRP wurden als erste ihrer Art für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt und durch den APEC-konformen Datenschutzmanagement-Anbieter TrustArc erworben und unabhängig validiert.

5.5. Rückgabe und Löschung von Kundeninhalten

Kunden von GoTo-UCC-Lösungen können jederzeit einen Antrag auf Rückgabe oder Löschung ihrer Inhalte stellen. Derartige Anträge werden innerhalb von dreißig (30) Tagen nach Antragstellung (oder früher, wenn dies nach geltendem Recht erforderlich ist) erfüllt. Darüber hinaus werden die Meeting-Chronik und die Cloud-Aufzeichnungen von GoTo Meeting während der aktiven Abonnementlaufzeit des Kunden automatisch auf einer rollierenden Basis von einem (1) Jahr gelöscht.

Nach Beendigung eines kostenpflichtigen Abonnements für GoTo Meeting werden die Konten des Kunden wieder zu kostenlosen Konten umgewandelt. Wenn ein Konto ausdrücklich gekündigt oder aufgelöst wird, werden die Inhalte innerhalb von 90 Tagen nach der Kündigung oder Auflösung gelöscht. Für kostenlose GoTo-Meeting-Konten gilt derselbe rollierende Zeitplan für die Löschung nach einem Jahr wie oben beschrieben. Darüber hinaus werden kostenlose GoTo-Meeting-Konten nach zwei (2) Jahren Inaktivität des Benutzers (z. B. keine Anmeldungen) automatisch gelöscht.

Um die saisonale Nutzerbasis zu berücksichtigen, werden GoTo-Webinar- und GoTo-Training-Konten zwei (2) Jahre nach Ablauf oder Auflösung der letzten Laufzeit gelöscht. GoTo-Stage-Benutzer können veröffentlichte Webinare während eines aktiven GoTo-Webinar-Abonnements jederzeit eigenständig über die GoTo-Webinar-Dienstumgebung und/oder durch Einreichen einer Support-Anfrage an GoTo zurücknehmen/entfernen. Auf schriftliche Anfrage wird GoTo die Löschung des entsprechenden Kontos und der Inhalte bestätigen.

5.6. Vertrauliche Daten

Obwohl GoTo bestrebt ist, alle Kundeninhalte zu schützen, sind wir aufgrund regulatorischer und vertraglicher Bestimmungen dazu gezwungen, die Verwendung von GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage für bestimmte Arten von Informationen einzuschränken. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage hochgeladen oder generiert werden:

- Von der Regierung ausgestellte Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen, die sich auf die Gesundheit einer Person beziehen, einschließlich, aber nicht beschränkt auf geschützte Gesundheitsinformationen (Protected Health Information, PHI) gemäß Definition im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) und verwandte Gesetze und Vorschriften.
- Informationen im Zusammenhang mit Finanzkonten und Zahlungsinstrumenten, einschließlich, aber nicht beschränkt auf, Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung bezieht sich auf ausdrücklich gekennzeichnete Zahlungsformulare und -seiten, die von GoTo verwendet werden, um Zahlungen für GoTo Meeting, GoTo Training, GoTo Webinar und GoTo Stage einzuziehen.
- Alle Informationen, die durch geltende Gesetze und Vorschriften besonders geschützt sind, insbesondere Informationen über Rasse, ethnische Zugehörigkeit, religiöse oder politische Überzeugung, Mitgliedschaften einer Person in Organisationen usw.

5.7. Tracking und Analyse

GoTo verbessert seine Websites und Produkte kontinuierlich mithilfe von Webanalyse-Tools von Drittanbietern, die GoTo dabei helfen, zu verstehen, wie Besucher seine Websites, Desktop-Tools und mobilen Anwendungen nutzen und welche Benutzereinstellungen und Probleme sie haben. Weitere Informationen entnehmen Sie bitte der Datenschutzrichtlinie.

6 Drittanbieter

6.1. Einsatz von Drittanbietern

Im Rahmen der internen Beurteilung und der Prozesse in Bezug auf Anbieter bzw. Drittanbieter können Anbieterbeurteilungen je nach Relevanz und Anwendbarkeit von mehreren Teams durchgeführt werden. Das Sicherheitsteam evaluiert Anbieter, die auf Informationssicherheitsdienste anbieten, dazu gehört auch die Beurteilung von Hosting-Einrichtungen Dritter. Die Rechts- und Beschaffungsabteilungsteams können Verträge, Leistungsbeschreibungen (Statements of Work, SOW) und Dienstleistungsvereinbarungen nach Bedarf im Rahmen interner Prozesse beurteilen.

Angemessene Unterlagen oder Berichte über die Einhaltung der Vorschriften können mindestens einmal jährlich eingeholt und ausgewertet werden, um sicherzustellen, dass das Kontrollumfeld angemessen funktioniert und alle notwendigen Kontrollen zwecks Berücksichtigung der Benutzer durchgeführt werden. Darüber hinaus müssen Dritte, die sensible oder vertrauliche Daten von GoTo hosten oder von GoTo Zugang zu diesen gewährt wird, einen schriftlichen Vertrag unterzeichnen, in dem die entsprechenden Anforderungen für den Zugang zu, die Speicherung oder den Umgang mit den Informationen (je nach Fall) dargelegt sind.

6.2. Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität der Geschäftsprozesse und der Datenverarbeitung Dritter getroffen werden, prüft GoTo die Geschäftsbedingungen der betreffenden Dritten und verwendet entweder von GoTo genehmigte Beschaffungsvorlagen oder handelt die Bedingungen dieser Drittanbieter aus, sofern dies für erforderlich gehalten wird.

7 Kontaktaufnahme mit GoTo

Kunden können GoTo unter https://support.goto.com für allgemeine Anfragen oder privacy@goto.com für Fragen zum Datenschutz kontaktieren.